E_Universities Services in the New Social Eco-systems:

Using Conversational Agents to Help Teach Information Security Risk Analysis

Stewart Kowalski, Robert Hoffmann, Rohan Jain, Majid Mumtaz
Department of Computer and Systems Sciences, Stockholm University,
Stockholm, Sweden
stewart@dsv.su.se, robe-hof@dsv.su.se, roha-jai@dsv.su.se, mmumtaz@dsv.su.se

Abstract— **New social eco-systems and globalization are creating new challenges to educational institutions. Teachers need now not only to consider personal differences among their students, but also to take care of different cultural behaviors. Teachers are now expected to provide both a standardized and individual knowledge transfer to their students. This conflict may be resolved by utilizing results from artificial intelligence research, in particular chat bots. By giving the teacher a virtual assistant who can take care of the basic knowledge provisioning, the teacher has more freedom to handle the complex situations. In this paper we provide a short overview of relevant research that we used to build our own knowledge bot. The results from using the bot in teaching a undergrad class in Sweden is presented, together with an analysis and some suggestions for future work.**

Keywords -AI; knowledge bot; learning; teaching

I. INTRODUCTION

New and developing global social eco-systems are creating new challenges for educations institutions. The globalization of knowledge creation and transfer now means that educational institutions now must compete for students from around the world. These global students expect definitive answer and to be educate anywhere and at any-time. University educators now must not only adapt their teaching to different learning styles they must also take care of different cultural behaviours and in real time. In this paper, we describe an attempt to deal with the problem faced by these new e-learners as they learn to us an artificial intelligent conversational agent to assist in teaching a course in information security organization and management. Students were given the opportunity during the course to work with the courses content either via a wiki page moderated by a teaching assistant or through discussion with the AI conversational agent. Findings from the analysis of the student activity logs suggest that most of the students seem to preferred the AI conversational agent to the wiki work process.

In the first part, we will describe the theoretical aspects of using bots in teaching and existing research. The second part discusses our own bot and our experiences from using it. The paper ends with a conclusion and suggestions for further work.

II. THEORETHICAL ASPECTS

A. Cultural issues in teaching

As a result of increasing globalization, we live in a world where we are surrounded by people of different origins with their own different cultures. Universities are a good example of such a place where we encounter people from different parts of the globe working and interacting in the same environment. To work with such an international audience as a teacher and express ones own thoughts and ideas is a challenge in itself. An even bigger problem however arises when the audience needs to interact with the teacher by bring forward their own opinions and questions.

We have observe during lectures that, whenever a teacher poses an open question in front of the class, that a large majority of the students remain silent. Research that was done in the USA [1] indicated that culture plays a vital role in influencing how a individuals is either too open or too shy towards the world. For example, in Asian countries, people tend to be much shyer as compared to those in western occidental countries. One of the possible rationalizations behind this fact is that most of the times, a person's success is credited externally to his family, parents, teacher or others, while his failure is entirely blamed on him.

B. Chat bots

A chatterbot, chatbot or conversation agent is a software program developed to imitate human like conversation, either in text form or via audio. This fast growing technology already plays an important role in various fields such as help desk tools or customer support. Some chat bots provide online help, personalized services and information acquisition services, which requires them to be rather sophisticated in processing natural language. But the common technology is based on pattern matching such as those of the ALICE systems, which use the AIML computer language [2].

Chat bots can play a useful role for educational purposes, because they are an interactive mechanism as compared to traditional e-learning systems. Students can continually interact with the bot by asking questions related to a specific field. Although chat bots have been around since the middle of 1960's, only few of them have been used for educational purposes and all were related to specific subjects. The Virtual Patient bot (VPbot) is an example of an educational bot used at the Harvard Medical School. Medical students

ISBN: 978-1-61208-163-2

could interact with the bot and asked him for medical knowledge, whereupon the VPbot would answer them via audio or text [3].

Another Chat bot used for educational purposes was Sofia [4]. It was developed for the mathematics department of Harvard. The main purpose of this bot was to teach algebra. Students interacted with Sofia by asking specific questions related to mathematics and teachers could at the same time improve the bot's knowledge. This was done through analysing the chat logs to see which types of questions the students asked frequently and which questions needed better answers. This analysis was not only very helpful in improving the bot, but also the teachers improved their teaching patterns in classes as well [3][4].

C. Use of bots in learning and information

1) Advantages of using bots

Chat bots are not only an interesting way of providing knowledge to the audience, but they can also be the enabler to allow the audience to participate. By talking to a neutral entity the students might be less inhibited and will show more participation. An experiment where a chat bot was used to teach English as a foreign language resulted in 85\% of the students preferring the bot over a human teacher [6].

The bot can also help the teacher to become more efficient. By answering recurring questions and providing basic knowledge it can take a certain amount of the workload away and thereby enable the teacher to focus on more specialized or complicated questions. Furthermore can the bot collect anonymous questions and forward them to the teacher. This lowers the barrier for the students to ask questions and bring in opinions.

2) Creating believable bots

For a bot to seem real and thereby accepted as a conversation partner he has to behave in a social way. Previous research in this area [7] tries to show how one can make the bot more realistic and believable during a conversation by adding some parameters related to general awareness. The authors demonstrate different kinds of parameters that define environmental, self and interaction awareness in the conversational agents. To test their theory, they performed an experiment where the test users were made to interact with some conversational agents as well as humans in a virtual world simulation and hence had to deduce if they were talking to a human or a robot. Their experiment was quite successful and demonstrated that it was much more difficult for the participants to differentiate between an aware conversational agent and a human. Hence, it was concluded that by adding such parameters to an agent, we can create a strong and much more believable bot tool for effective conversations.

3) Two corporate case studies

One of the authors has previously evaluated the use of chat bots for security training in an enterprise environment [8].

In the first case study the design and usage of a chat bot was investigated from an end user perspective. The author conducted a survey by dividing the end users into two groups. One group was given the chat bot while the other group was exclusively using an e-learning product. The main goal of the education was to teach knowledge, attitude and behavior in regard to security issues. As the result of this case study it was shown that the group which had used the chat bot showed better results than the e-learning users. It can therefore be concluded that the chat bot was the more effective technology for creating security awareness among users.

The second case study was performed on security specialists. They were divided into two groups and one was asked to use the bot for a period and then post their views about information they got from it. Although both groups showed the same level of knowledge afterwards, the group that used the bot reported a better learning experience and was eager to use it again.

4) Using bots in the classroom

The paper by Knill investigates the benefits and risks in pedagogic environment [4]. The main aim of using media and technology in classroom is to provide interaction choices for students and teachers, and also to have access to knowledge 24x7. But there are also risks. If used inappropriately in the classroom, the technology can be used to perpetuate the old model of teaching and learning. And there are also new risks such as equipment failures, bugs in software and hardware, security vulnerabilities, compatibility issues, and human issues.

The Freudbot is another example of a successful bot usage [9]. The aim of this text based chat bot was to let psychology students interact with a virtual Sigmund Freud. They could discuss Freudian concepts, theories and biographical events. It was an attempt to use technology for improving distance education. In the survey that was taken after the experiment the students gave a very positive feedback and especially valued the feeling of talking to the real Freud.

5) Pedagogical challenges

New technology cannot simply be introduced into a learning environment, but rather has to be adapted to the needs of the student and the teacher, as Laurillard shows in her paper [10]. She explains that in order to exploit the technology in teaching, we need to define the different pedagogical challenges. She also considers how the needs of both teachers as well as learners can be represented with respect to collaborative learning and hence provides a "Conversational Framework" explaining how one can use a pedagogical framework and integrate it with technology to deliver an interactive and genuinely enhanced learning environment for people. The full framework embraces all the elements prioritized by each of the main pedagogic approaches such as instructionism, constructionism, social learning and collaborative learning and demonstrates the complexity of what it takes to learn: a continual iteration between teachers and learners, and between the levels of theory and practice.

6) Automated social engineering

Unfortunately can bots also be misused as Huber shows in his master thesis [11]. Social engineering attacks are prevailing these days in the internet world via various social networking services such as Facebook, MySpace etc. In his thesis, the author describes different principles that are involved along with various techniques adapted by the attackers. But his main task was to perform an automated social engineering attack on an organization using a chat bot. To conduct the experiment, the author created two fake profiles called "Julian", managed by a human and "Anna", a chat bot. A group of test persons were instructed about the experiment and then had to communicate with a randomly chosen profile. Their task was to deduce if they were communicating with the human or the bot.

The results showed that the users were able to differentiate successfully between a human and machine. However, this thesis also showed that social engineering attacks are possible today and can pose a serious threat to an organization. This kind of threat is relatively new and no strong security measures are adopted by companies to handle them.

III. Using a Bot to Teach Risk Analysis

Similar to the Sofia bot and Freudbot, our team developed a bot for information security students, called Octavius. He was used as an aid in teaching the OCTAVE risk analysis method [12], hence his name.

The whole system is web based and consists of the chat bot and also a Wiki site. The bot itself is based on the ALICE system and therefore AIML. But it was extended to be able to open Wiki pages as part of the answer, if appropriate. This allowed the bot to give short and precise answers, but at the same time also provide in depth information through a Wiki page.

The students were introduced to the bot at the beginning of the 10 weeks course, and its knowledge was improved over time through a continuous log file analysis. All participants were aware that their conversations and IP addresses were logged, but also that there was no interest in identifying the actual users. This created an anonymous environment in which the students could openly chat with the bot.

Also had the students the choice of using the bot, only the Wiki or neither.

A. *Technical environment*

The client side was written in HTML and JavaScript and served through a regular Apache web server using HTTPS.

The server side bot engine was written in Python, based on the PyAIML interpreter [12] by Cort Stratton. It was extended with multi-processor capabilities, load balancing and statistics generation.

OpenBSD 4.8 (http://www.openbsd.org) was used as the operating system, running on an Intel quad-core CPU. This gave a sustained performance of more than 20 answered questions per second and less than 0.2 seconds answer time per question, which resulted in an immediate feedback for the user.

The default AIML set as provided by the ALICE project [2] was slightly modified and extended with specific OCTAVE knowledge.

B. *Student reactions*

63 sessions were done with the bot, in which he was asked 510 questions. The median session time was 35 seconds. Based on the evaluated log files we can see that this resulted often from insufficient flexibility of the bot. The users often could see that they were talking to an artificial being. It is planned to mitigate this effect in the future through refined AIML sets. One of the main problems in this regard is from our experience the balance between small talk and specific know how. Too much of the former results in a bot without value, whereas too little of it makes the bot seem unnatural.

But still the bot provided a positive learning experience for the students. While they had the choice between the bot or the Wiki alone, nearly all of them preferred to talk to the bot. This shows that the provisioning of such a system alone already encourage interest in it.

During an informal discussion with the students after the course, the general feedback was positive. They encouraged the usage of the bot, given that the knowledge base is improved so that he becomes more valuable in terms of a time spent versus knowledge gained decision.

C. *Conclusion*

There will be an increasing demand for IT based teaching, especially on university in the new developing social eco-systems. The different cultural backgrounds, and therefore learning styles and behaviors, require the teacher to focus more on the needs of his students. Given his limited time and resources, this can be supported by moving the task of basic knowledge transfer to an automated system or knowledge bot. This allows him to spend his efforts on high value interactions and newly upcoming questions, while still providing all necessary knowledge to his class.

We have shown by various examples that students can benefit from such a system and usually are very open minded in using it. But still a considerable effort has to spend on creating such a system in a way that makes it look real to the audience.

1) *Future work*

We will continue to improve Octavius, and at the same time branch off the system into other bots for different subjects. On the theoretical side have we identified the need for research into utilizing AIML. Only by fully exploiting the possibilities of the language will it be possible to create realistically behaving ALICE bots.

References

[1] L. Henderson and P. Zimbardo, “Shyness”, Encyclopedia of Mental Health, 1996.

[2] R. Wallace, “Artificial Linguistic Internet Computer Entity”, The A.L.I.C.E. AI Foundation, 1995.

[3] B. A. Shawar and E. Atwell, “Chatbots: Are they Really Useful?”, LDV-Forum, vol. 22, pp. 22-49, 2007.

[4] O. Knill, and J., Carlsson, Andrew Chi and Mark Lezama, An artificial intelligence experiment in college math education, http://www.math.harvard.edu/~knill/preprints/sofia.pdf,, accessed, Sept 2011.

[5] O. Knill, “Benefits and Risks of Media and Technology in the Classroom”, ICTCM, 2007.

[6] L. Fryer and R. Carpenter, “Emerging Technologies: Bots as Language Learning Tools”, Language Learning & Technology, nr. 3, vol. 10, pp. 8-14, 2006.

[7] B. Reeves, “The Benefits of Interactive Online Characters”, Stanford University, 2000.

[8] S. Kowalski, K. Pavlosvska and M. Goldstein, “Two Case Studies in Using Chatbots for Security Training”, Royal Institute of Technology Stockholm, 2009.

[9] B. Heller, M. Procter, D. Mah, L. Jewell and B. Cheung, “Freudbot: An Investigation of Chatbot Technology in Distance Education”, Athabasca University, Canada, 2005.

[10] D. Laurillard, “The pedagogical challenges to collaborative technologies”, Computer-Supported Collaborative Learning, vol. 4, pp. 5-20, 2009.

[11] M. Huber, “Automated Social Engineering: Proof of Concept”, Royal Institute of Technology Stockholm, 2009.

[12] OCTAVE, http://www.cert.org/octave, access ed Sept 2011.

[13] C. Stratton, PyAIML, http://pyaiml.sourceforge.net, acessed Sept 2011.